



Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute mõistmise ja nendega toimetuleku ülevaade

Ennetavad tegevused

Safeguarding against Phishing in the age of 4th Industrial Revolution

www.cyberphish.eu

This project has been funded with support from the European Commission.

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Õppe-eesmärgid



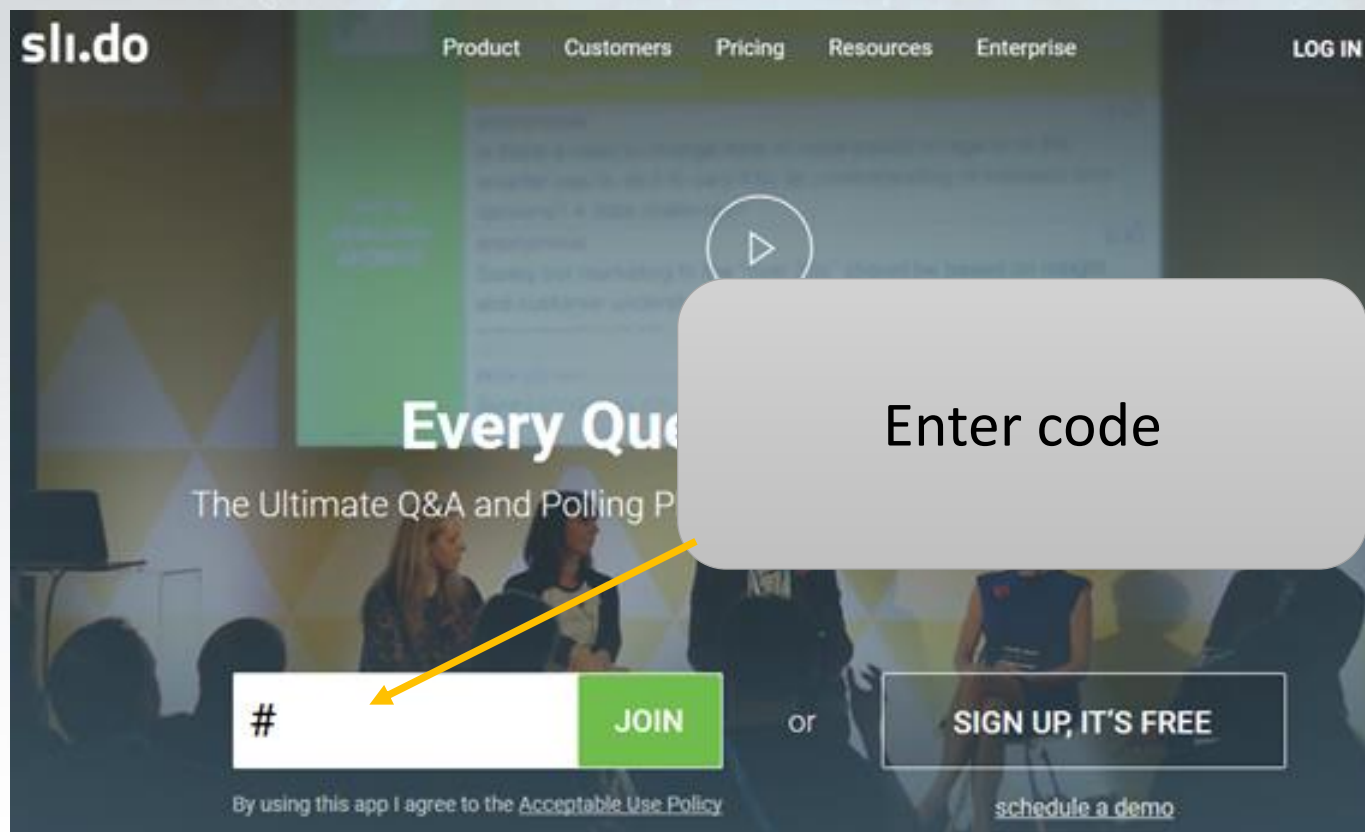
Küberhügieen Internetis
Küberhügieen töökohal
Tehnoloogilised vahendid ja meetmed

Õpilase töökoormus



Loengud	2 h
Audio- ja videomaterjal	1 h
Juhtumiuuringud	0,5 h
Lisalugemine	1,5 h
Eksamiks valmistumine	1 h

Praktiline harjutus: palun sisesta sli.do keskkonnas võimalikult palju omadussõnu, mis on seotud interneti ja digiseadmete turvalisusega





Küberhügieen Internetis

USERNAME:

Administator

PASSWORD:

•••••

LOGIN

Digitaalne jalajälg

- Teave, mis on salvestatud kasutaja toimingute kohta: külastatud veebi-saidid, vaadatud profiilid või fotod, täidetud vormid, registreerumised kohtingusaidil, installitud rakendused jne.
- **Aktiivne jalajälg** - teave, mille me vabatahtlikult ja teadlikult üles laadime ja maha jätame (fotod, postitused, kommentaarid)
- **Passiivne jalajälg** – teave, mille jätame endale teadvustamata, sageli isegi teadmata või mõistmata (IP-aadress, otsinguajalugu, geograafilise asukoha andmed)



Personaalne informatsioon

Isikuandmed on teave, mis määratleb seose konkreetse teabe ja isiku vahel.*



* *Malinauskaitė-van de Castel, Inga. Data subjects' rights in virtual social networks: doctoral thesis. – Vilnius, 2017.*

Mis on isikuandmed?

- Isiku kontaktandmed (nt nimi, perekonnanimi, kodune aadress, mobiilnumber)
- Biomeetrilised andmed
- Isikukood
- Isiku ID- või passikood
- Isiku sissetulek
- Paroolid
- Finantsandmed
- Klientide andmed
- Intellektuaalsed andmed ilma omanike loata



Mis on avalikud andmed?

- Avalikud andmed on näiteks:
 - Ettevõtte kood
 - Ettevõtte e-posti aadress, näiteks info@company.com
 - Anonümiseeritud andmed
 - Hüüdnimi
 - Hobid
 - Loodusfotod
 - Blogid
 - ...



Miks on oluline isikuandmeid mitte avaldada?

- Identiteedivargus
- Küberkuriteod (vargused, väljapressimine, ahistamine)
- Võimalik maine kahjustamine:
 - Igaüks Internetis võib vabalt saada-olevatele andmetele juurde pääseda
 - Avaldatud andmeid kasutatakse isiku vastu
- Mida rohkem teavet Internetis avaldatakse, võivad petturid varastada isiku identiteeti, kasutada and



Kontrollige, milline teave on teie kohta saadaval

- Kasutage otsingumootorit, et otsida ennast internetist ja vaadata, millist teavet leiata
- Kontrollige enda kohta teavet erinevate otsingumootorite abil
 - Google
 - Bing
 - DuckDuckGo
- Kasutage otsingu tegemiseks tsitaate ja muid sümboleid, näited:
 - "Perekonnanimi" – saate selle inimese kohta teavet
 - "Nimi Perekonnanimi@" – saate selle inimesega seotud e-kirju
 - "Nimi perekonnanimi" failitüüp: PDF – teie PDF-dokument, kus seda isikut mainitakse

Fotode avaldamine

- Kas olete mõelnud:
 - Kellel on juurdepääs teie fotodele?
 - Kas fotol on teisi inimesi?
 - Kas fotole on salvestatud GPS-teave asukoha kohta?
- Otsingumootori abil saate proovida endast fotosid leida



Fotode ja videode jagamine

- Austage teiste inimeste privaatsust
- Kui soovite jagada fotot või videot tuttavate inimestega, on hea kombeks küsida luba
- Ärge levitage fotosid teiste inimeste lastest ilma nende vanemate loata
- Ärge kasutage oma reklaammaterjalides inimeste fotosid, kui nad pole selleks luba andnud
- Pildistage võõraid inimesi ainult avalikus kohas. Kui isik on sõnaselgelt teatanud, et ta ei soovi, et teda pildistatakse, ei saa te teda pildistada
- Ärge jagage fotosid ja videoid kättemaksu või mõnitamise vahendina
- Ärge jagage vägivaldseid, vaenu õhutavaid või solvavaid fotosid ja videoid. Isegi kui soovite vägivalla või vihkamise hukka mõista
- Ärge jagage fotosid ja videoid, kus teid või teie sõpru või sugulasi tabatakse reeglite rikkumise, sobimatu käitumise või isegi seaduste rikkumisega

Fotode ja videode jagamine

- Kui leiate enda või oma lähedaste foto ja te ei soovi, et seda jagataks, võiksite võtta kasutusele järgmised meetmeid:
 - Võtke ühendust väljaandjaga ja taotlege eemaldamist
 - Võtke ühendust sotsiaalsõrgustiku administraatoriga ja paluge foto eemaldada, selgitades olukorda
 - Kui ülaltoodud sammud pole aidanud, pöörduge isikuandmete kaitse inspektsiooni poole.

Sõbrad sotsiaalvõrgustikes

Olge nutikas ja valiv, kui võtate kasutajaid sotsiaalvõrgustikes sõbraks



Hoiduge oma isikut tuvastava teabe avaldamisest

- Kõik, mida Internetti paned, võib olla püsiv
- Teave võiks olla saadaval arhiivides, st <https://web.archive.org>
- Teised inimesed võivad
 - salvestada teavet oma seadmetesse
 - printida või
 - teabe uuesti avaldamine Internetis

Jälgige, millist teavet teie kohta Internetis avaldatakse

- Saate jälgida, kas veebilehtedel, ajaveebides, teadusuuringutes, foorumites, Youtube'is avaldatakse kasutaja kohta uut teavet, kasutades muudatuste tuvastamise ja teavitamise teenuseid, nagu Google Alerts.
- Google Alert süsteemis on võimalik esitada märksõnu
- Kui leitakse uued tulemused, saadetakse kasutajale teavitusmeil või kasutaja saab tulemusi igal ajal vaadata aadressil www.google.com/alerts



Isikuandmete Google'i teenustest eemaldamise taotlus

- Täieliku teabe esitamisel võite teatada, et teid käsitlev sisu eemaldatakse Google'i teenustest
- Võite taotleda sisu eemaldamist Google'i teenustest:

- ☐  Google Search
- ☐  Blogger/Blogspot
- ☐  Google Maps and related products
- ☐  Google Play: Apps
- ☐  YouTube
- ☐  Google Images
- ☐  A Google Ad
- ☐  Drive and Docs
- ☐  Google Photos and Picasa Web Albums
- ☐  Google Shopping
- ☐ See more products

Kontrollige, kas teie andmeid on lekkinud

- Saate kontrollida, kas teie e-posti või telefoni teel on andmekaitsega seotud rikkumine, kasutades veebitööriistu, nagu Have I Been Pwned? <https://haveibeenpwned.com/>
- Samuti saate kontrollida, kas teie parool lekkis <https://haveibeenpwned.com/Passwords> . Lekkinud paroolid on veebis otsitavad ja igaüks saab neid alla laadida

';--have i been pwned?

Jälgige andmete lekkimist

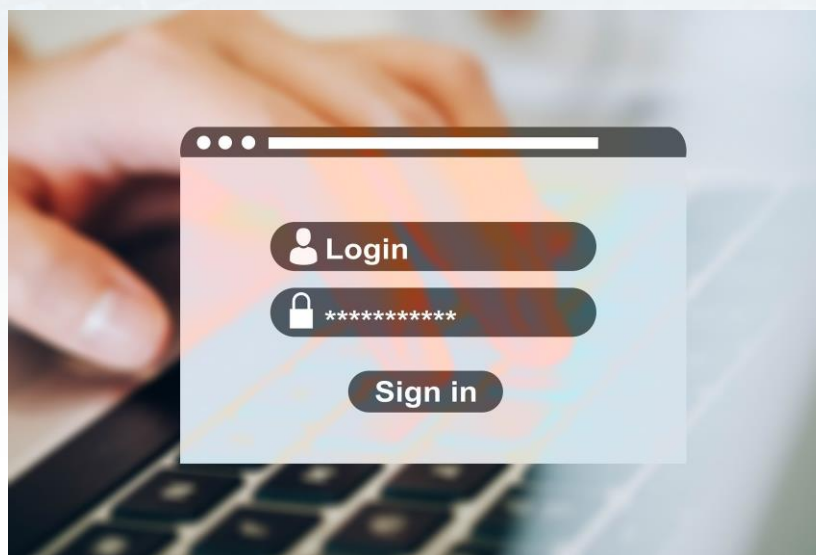
- Registreeruda saab spetsiaalsetes portaalides, mis annavad teada, kui kasutajakonto on lekkinud, näiteks: <https://monitor.firefox.com>



More information: www.cnet.com/tech/services-and-software/firefox-monitor-shows-if-your-personal-information-was-lost-in-a-hack
<https://www.online-tech-tips.com/computer-tips/what-is-firefox-monitor-and-how-it-protects-your-login-details/>

Toimingud, kui teie konto lekkis

- Kui teie andmed lekkisid, tähendab see, et teie e-post ja parool võivad olla küberkurjategijate käes. Sellisel juhul peaksite
 - muutke viivitamatult oma sissemurtud konto parool
 - muutke teiste kontode parooli, kui kasutasite sama parool
 - lubage kahefaktoriline autentimine, kui tarkvara seda toetab



Vältige isiklike andmete jagamist

- Kasutajad peaksid olema ettevaatlikud teabe avalikustamise osas, sest tavaliselt kipuvad inimesed liialt teavet sotsiaalvõrgustikes jagama
- Ärge avaldage enda plaane, koduseid aadresse, finantsteavet
- Kohandage oma konto turvaseadeid ja hallake, kes näevad teie postitusi ja muud teavet



Kasutage erinevatel eesmärkidel erinevat e-maili postkasti

- Meil isiklikuks eluks, nt nimi.perekonnanimi@gmail.com
- Meil ärilistel eesmärkidel, nagu nimi.perekonnanimi@comapny-name.com
- Registreerumise e-kiri
 - saate luua konto tasuta meiliteenuste portaalides registreerumiseks
 - võite kasutada ajutist meiliteenust, nagu Guerrilla Mail, Mailinator

Ärge usaldage, vaid kontrollige

- Olge ettevaatlik, kui klõpsate linke, mida saate oma sõpradelt sõnumites
- Ärge usaldage, et sõnum on tõesti saatjalt, kellelt see väidetavalt pärineb
- LUGEGE enne, kui klõpsate millelgi tasuta programmide allalaadimiseks või installimiseks



The background image features a person wearing a white face mask, rendered in a blue-tinted, semi-transparent style. Overlaid on this is a complex digital network of white lines and dots, resembling a globe or a data mesh. A white smartphone is positioned diagonally across the upper right portion of the image. The overall aesthetic is futuristic and technological.

Digiseadmete hügieen

Digitaalsete seadmete turvalisus

- Kasutajad peavad nii arvutit kui nutiseadmeid kasutades käituma vastutustundlikult ning kasutama vastavaid turvameetmeid, sest nutiseadmetel on sarnased funktsioonid laua- või sülearvutitega
- Nende seadmete kasutamine võib kaasa tuua samu turvaprobleeme nagu arvutid, andmekadu jne.
- Nutiseadmeid saab kaitsta ka viiruste ja muude potentsiaalsete võrguohutude eest nagu arvuteidki

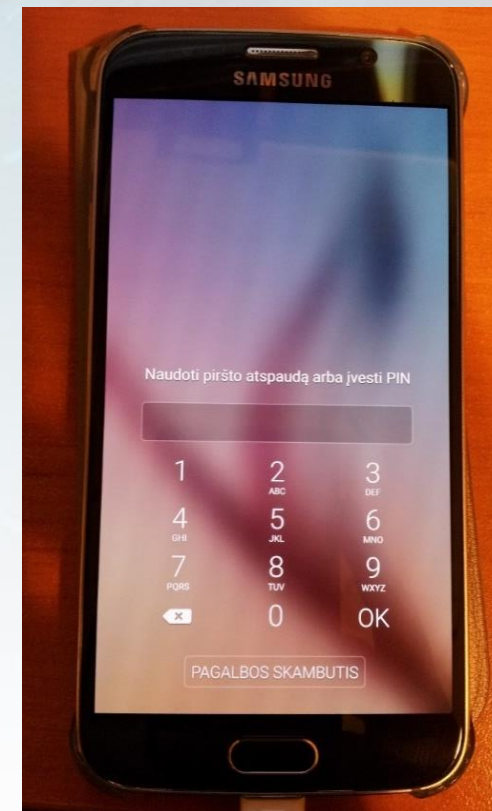
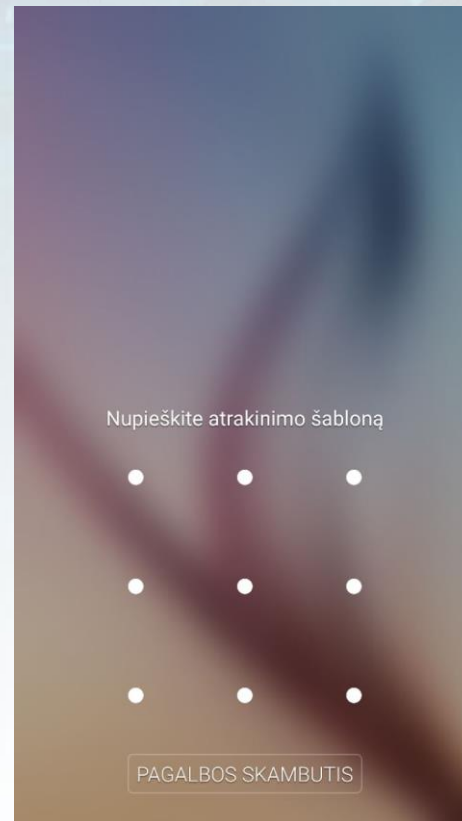


*Kasutage digiseadmetega ühenduse
loomiseks sisselogimisi ja paroole*



Aktiveerige PIN-koodi või muu turvalise sisselogimise funktsioon

- Mobiilseadmete puhul on soovitatav aktiveerida PIN-kood iga kord enne seadme kasutamist, et vältida volitamata isikute kasutamist, teie isiklike andmete, fotode jms vaatamist.
- Mõnel seadmel on ka muid turvalisi sisselogimise funktsioone, näiteks sõrmejälgede skannimine, silmade skannimine
- Lubage automaatne lukustusfunktsioon pärast seadmega töötamise lõpetamist



Privaatne sirvimine

- Keelake kolmanda osapoole küpsised
- Kasutage privaatset sirvimisrežiimi
- Kasutage brauseri lisandmooduleid (nt HTTPS Everywhere).
- Kui teil on vaja liiklust peita, kasutage virtuaalse privaatvõrgu VPN-lahendusi
- Vaadake, mida Google teie kohta teab
<https://myactivity.google.com/myactivity>

Paroolihalduse juhised

- Ärge jagage oma kasutajanimed ja paroole teistele isikutele, isegi oma kolleegidele
- Ärge kunagi salvestage oma paroole märkmetesse, memosse või failidesse arvutis või mobiilseadmes
- Ärge kasutage paroole, mis koosnevad nimedest, aadressidest, telefoninumbritest ja muudest kergesti äraarvatavatest sõnadest
- Kasutage erinevate kontode jaoks erinevaid paroole
- Parema turvalisuse tagamiseks muutke oma paroole perioodiliselt
- Kasutage oma paroolide kaitsmiseks paroolihaldureid, nagu Firefox Lockwise, NordPass, KeePass

Kontrollige parooli keerukust

The Password Meter

www.passwordmeter.com

safest9

Test Your Password	
Password:	●●●●●●
Hide:	☒
Score:	23%
Complexity:	Weak

MyPassword!5SafeAndStrong

Test Your Password	
Password:	12345678901234567890
Hide:	☒
Score:	100%
Complexity:	Very Strong

Nõuanded töökohalt lahkumiseks

- Töö lõpetamisel katkestage ühendus infosüsteemidega
- Brauseri sulgemine ei pruugi teid välja logida
- Lukustage oma digitaalne seade, kui olete seadmest isegi mõneks ajaks eemal. Kui jätate seadme lukustamata, võivad teised inimesed seda teha
 - Juurdepääs oma teabele ilma teie loata
 - Juurdepääs konfidentsiaalsetele andmetele
 - Saatke oma kontolt e-kirju
 - Kustutage oma failid
 - Tehke mõni muu pahatahtlik tegevus

Kui kasutate kellegi teise seadet

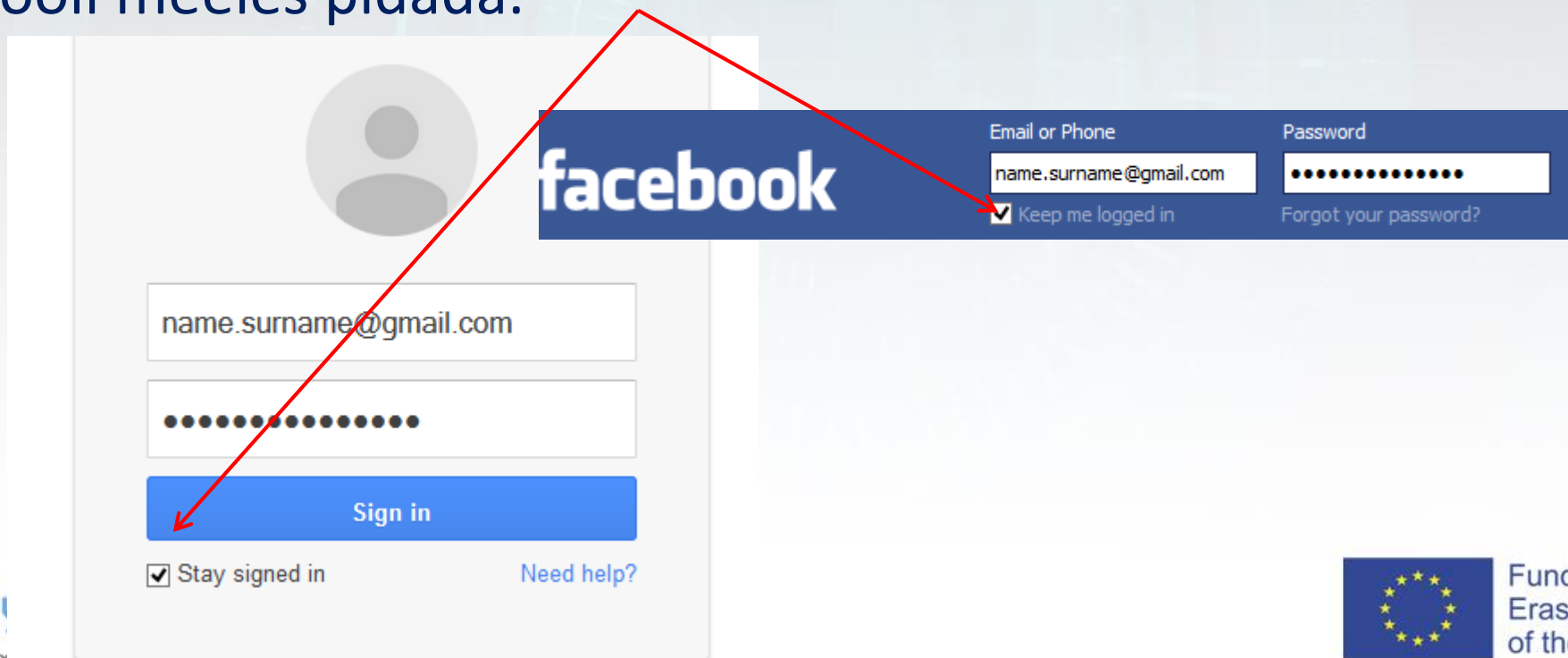
- Muutke kasutatud teenuse parooli usaldusväärsest arvutist ja võrgust, kui kasutate kellegi teise seadet ja kahtlustate ebatavalist tegevust
- Kasutage paroolide sisestamiseks "virtuaalset" klaviatuuri
- Logige välja veebisaitidelt, mis nõuavad autoriseerimist
- Ärge salvestage oma sisselogimisandmeid
- Kustutage oma Interneti-ajalugu ja allalaaditud failid

Kaitske end üle õla vaatamise vastu

- Kui töötate digitaalse seadmega, nagu arvuti, sülearvuti, nutitelefon, võib keegi üle õla vaadates jälgida, mida kasutaja ekraanil teeb, millist teavet või paroole sisestab, et saada teavet ja kasutada seda pahatahtlikeks tegevusteks.
- Enda kaitsmiseks üle õla vaatamise eest:
 - leidke ala, kus saate istuda või seista seljaga seina poole
 - Olge alati teadlik oma ümbrusest, mitte ainult inimestest, vaid ka videokaamerateist, mis võivad teie tegevust filmida.

Sisselogimine ja väljalogimine

- Kasutades avalikku arvutit (või kellegi teise seadet) tühjendage märkeruut „Hoia mind sisse logituna” või „Jää sisselogituks”.
- Ärge lubage veebibrauseril teie automaatseks sisselogimiseks teie parooli meeles pidada.



The image shows the Facebook login interface. A red arrow points from the 'Keep me logged in' checkbox to the 'Sign in' button. Another red arrow points from the 'Keep me logged in' checkbox to the 'Sign in' button.

facebook

Email or Phone
name.surname@gmail.com

Password
.....

☒ Keep me logged in [Forgot your password?](#)

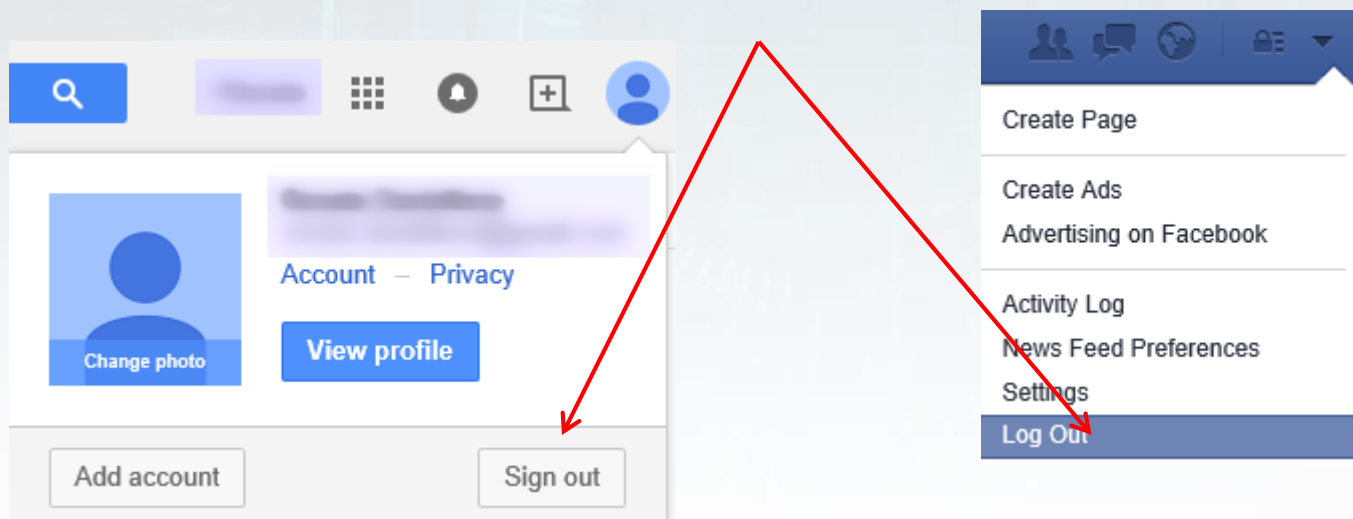
name.surname@gmail.com

.....

☒ Stay signed in [Need help?](#)

Sisselogimine ja väljalogimine

- Avalikku arvutit (või kellegi teise seadet) kasutades logige kontodelt ja rakendustest välja



Katkesta ühendus süsteemidega kaugjuhtimisega

- Saate kaugjuhtimisega välja logida, kui unustasite avaliku või kellegi arvutis kasutatud kontodelt välja logida või kui olete oma digiseadme kaotanud.
- Peate kontrollima, kas teenus pakub eemalt väljalogimise funktsiooni, näiteks Google, Facebook, Dropbox, Netflix, Microsoft, Instagram, Amazon jne.

Juhendid:

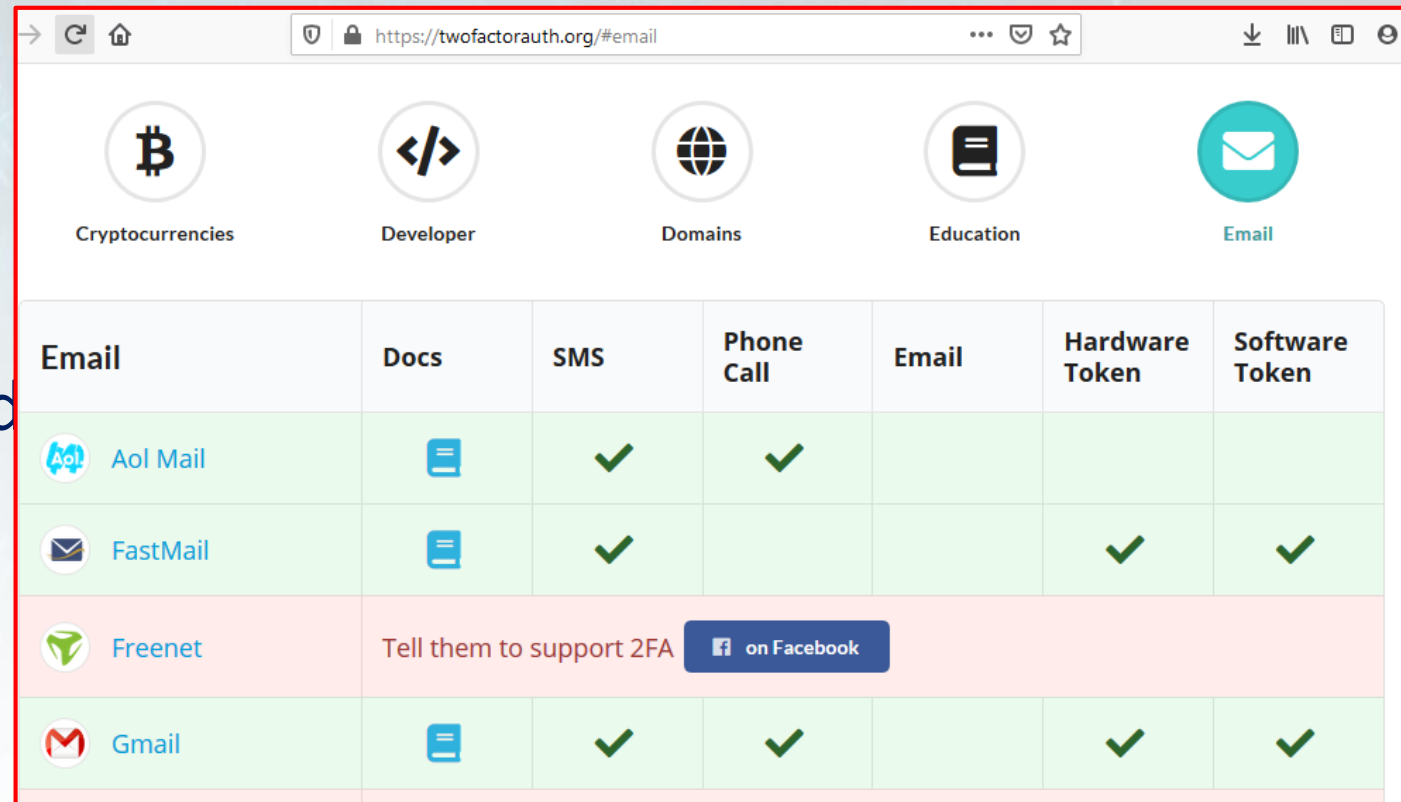
Sign-out from Google <https://support.google.com/mail/answer/8154?hl=en&co=GENIE.Platform%3DDesktop>

Sign-out from Netflix <https://help.netflix.com/en/node/18>

Sign-out from Dropbox <https://help.dropbox.com/accounts-billing/settings-sign-in/device-list-remote-sign-out>

Mitme astmeline autentimine

- Soovitav on lubada kahefaktoriline autentimine, kui teie teenusepakkuja seda toetab.
- Kontrollige, millised veebisaidid toetavad kahefaktorilist autentimist, <https://twofactorauth.org>



The screenshot shows the website <https://twofactorauth.org/#email>. At the top, there are five category icons: Cryptocurrencies (Bitcoin), Developer (code icon), Domains (globe), Education (book), and Email (envelope). Below these is a table with columns for different authentication methods: Email, Docs, SMS, Phone Call, Email, Hardware Token, and Software Token. The table lists several email services and their compatibility with these methods.

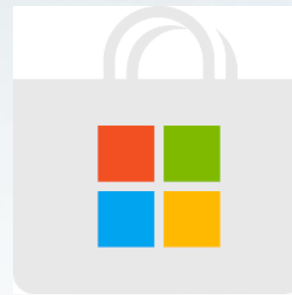
Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
Aol Mail		✓	✓			
FastMail		✓			✓	✓
Freenet	Tell them to support 2FA on Facebook					
Gmail		✓	✓		✓	✓



Tehnoloogilised probleemid

Installige juriidiline tarkvara ja rakendused ainult usaldusväärsetest allikatest

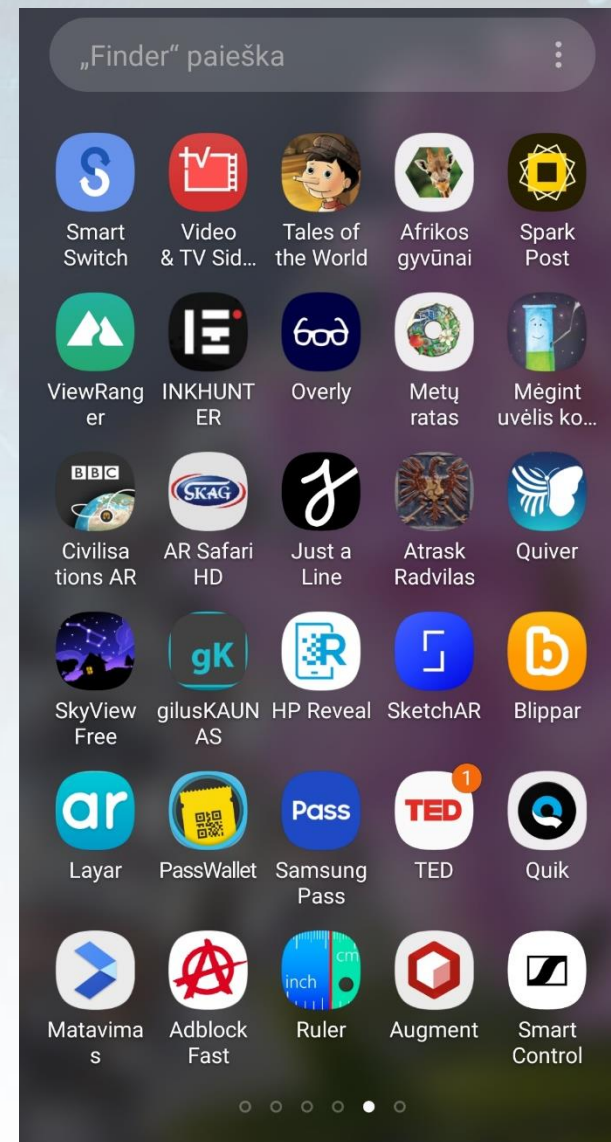
- Paigaldage seadmesse ainult legaalset tarkvara ja rakendused
- Ärge installige ebausaldusväärset tarkvara
- Installige rakendusi ainult usaldusväärsetest allikatest, näiteks:
 - Google Play
 - Apple App Store
 - Microsofti pood
 -



Google Play

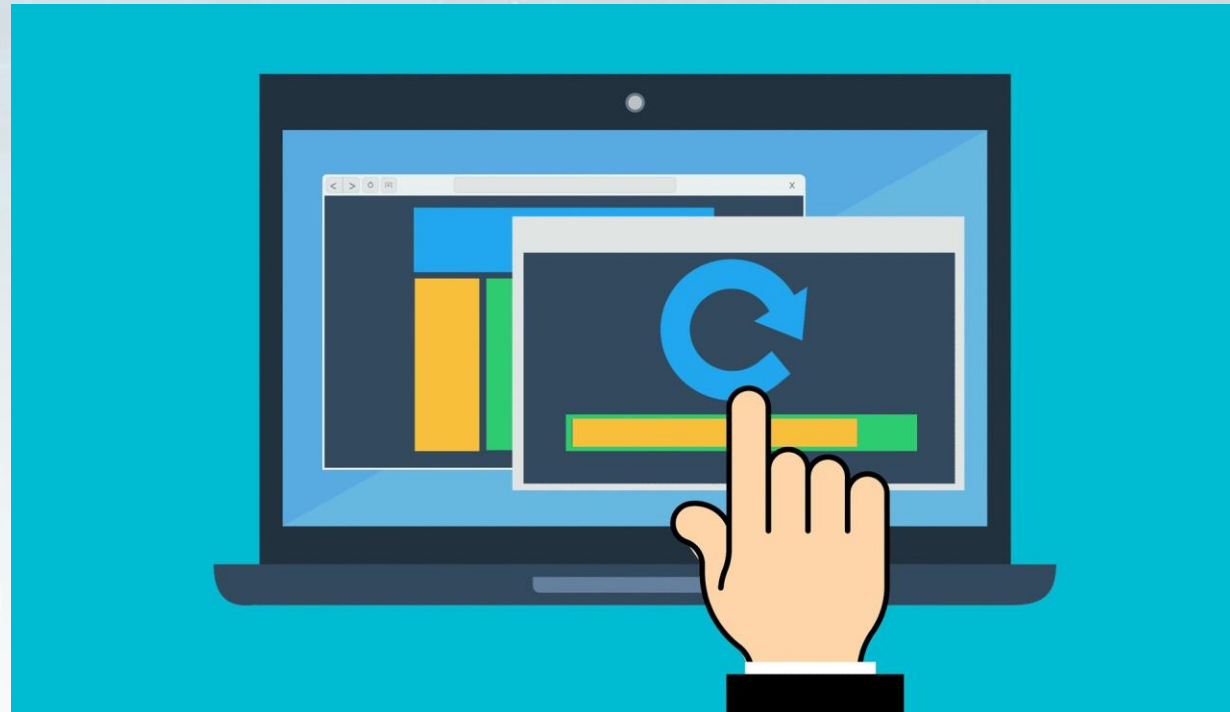
Küsimus

- Kas teate kõigi oma seadmes olevate rakenduste eesmärki?



Hoidke tarkvara värskendatud

- Veenduge, et seadmetesse, rakendustesse ja infosüsteemidesse installitakse regulaarselt kõik vajalikud värskendused ja parandused
- Lubage operatsioonisüsteemi ja tarkvara automaatsed värskendused



Kasutage viirusetõrje- ja Interneti- kaitsetööriistu

- Enamik viirusetõrjetarkvarasid on kaubanduslikud ja tasulised
- Isiklikuks kasutamiseks on saadaval mitmeid tasuta viirusetõrjeprogramme. Näited:
 - Avira tasuta viirusetõrje
 - AVG
 - Avast
 - Bitdefenderi viirusetõrje tasuta väljaanne
 - Windows Defender

Kasutage rämpsposti ja meilifiltreid

- Rämpspostifiltrid analüüsivad, tuvastavad ja peatavad soovimatud või ohtlikud meilid. Rämpspostifiltrid võivad e-kirju analüüsida erinevate kriteeriumide alusel
 - Päise filter
 - Sisu filter
 - Blokeerimisloendi filter
 - Reeglipõhine filter
- Rämpspostifilter hoiab ära serverite ülekoormamise ja ei lase töötajatel oma meilidele rämpsposti jõuda
- Peaksite teadma, et rämpspostifilter ei takista täielikult soovimatuid ja petturlikke kirju

Kasutage süsteemi krüptimise funktsiooni

- Süsteemi krüpteerimise funktsioon krüpteerib kõik teie telefonis või tahvelarvutis olevad andmed, sealhulgas rakenduste andmed, allalaaditud failid ja kõik muu
- Peate sisestama oma PIN-koodi või parooli iga kord, kui telefoni sisse lülitate



Varundage oma andmeid

- Andmete varundamine kaitseb teid arvuti krahhi või elektrikatkestuse või -tõusu korral, näiteks äikesetormi korral
- Kasutage varukoopiate tegemiseks välist kõvaketast või muud andmekandjat
- Varukoopiaid saab salvestada:
 - Välised salvestusseadmed
 - Interneti-draivid, nagu Dropbox, Apple iCloud, Google Drive jne.



Identiteedikaitse tööriist

- Kasutage hoiatusmärke, mis näitavad, et teie andmed on rikutud või teie kontole on sisse häkitud, näiteks Canary märgid.
- Canarytokens on tasuta tööriist, mis aitab teil avastada, et teid on rikutud, kuna ründajad on endast märgi maha jätnud.
- Canary token on fail, URL, API võti või muu ressurss, millele juurdepääsu jälgitakse. Kui ressursile on juurde pääsetud, käivitub hoiatus, mis teavitab objekti omanikku nimetatud juurdepääsust.



More information:

<https://canarytokens.org/generate> www.lacework.com/blog/canarytokensandransomwareoperations

Identiteedikaitse tööriist

- Canary token võivad olla
 - Veebiviga, URL-i luba (hoiatus, kui URL-i külastatakse)
 - DNS-i luba (hoiatus, kui küsitakse hostinime)
 - Unikaalne e-posti aadress (hoiatus, kui meil saadetakse unikaalsele aadressile)
 - MS Wordi, MS Exceli, PDF-failide märgid (hoiatus dokumendi avamisel)
 - Windowsi kaust (hoiatus kausta avamisel)
 - Jne.



More information about tokens generation:

<https://canarytokens.org/generate>

Nutiseadmete turvalisus

- Kontrollige ja konfigureerige kõigi rakenduste õigusi ja privaatsusseadeid
- Lubage kaughaldus ja andmete hävitamine
- Varundage oma mobiilseadme andmed
- Lülitage Bluetooth välja, kui seda ei kasutata
- Olge avalikes kohtades telefonis teabe vaatamisel ettevaatlik
- Lähtestage seadme tehaseaseaded enne selle müümist

Seadme ja võrgu kaitse

- Hävitage seadmed või mälupulgad, mida enam ei kasutata.
- Soovitatav on luua ühendus ainult usaldusväärsete traadita võrkudega, mis on kaitstud paroolidega.
- USB ja muu meedia krüpteerimine.
- Isikuandmeid sisaldavad dokumendid kustutage õigesti (jäädavate ehk püsivalt).

Muud soovitused

- Vältige P2P-d ja hajutatud failide jagamist
- Laadige failid alla seaduslikult
- Vältige veebilehtedel surfamist, mida te veel ei tea
- Vältige pakkumisi, mis on liiga head, et tõsi olla

Kõige olulisem vastukaal küberkurjategijatele: tarbijate teadlikkus ja valvsus!

Kasulikud teemaga seotud lingid

What is personal information? | Personal data

<https://www.cloudflare.com/en-gb/learning/privacy/what-is-personal-information/>

Video about how it is easy to get hacked: https://youtu.be/1hpU_Neg1KA

What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More

<https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more>

What is a digital footprint? And how to protect it from hackers <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>

How to Protect Your Digital Privacy

<https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy>

How to Remove Personal Information From the Internet

<https://www.lifelock.com/learn-identity-theft-resources-remove-personal-information-from-the-internet.html>

Ennetavad tegevused

- Küberhügieen Internetis
- Digiseadmete hügieen
- Tehnoloogilised probleemid



Ülesanne

Täida küsimustik:

- nimi, perekonnanimi,
- e-posti aadress,
- kooli nimi, mille sa lõpetasid,
- teie loomade nimed

TIP: You can use Google Form, but make sure the task is precise, for example, <https://forms.gle/uckbLqBmY2mkFs93A>

Üleasanne



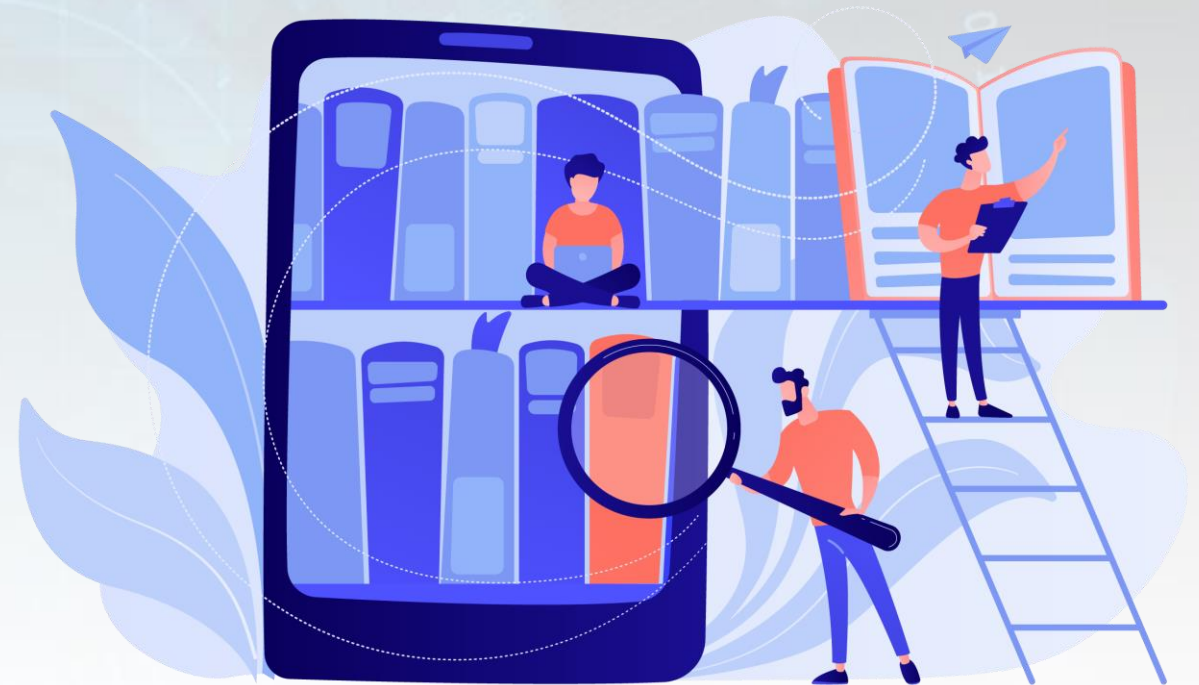
Arutage:

- Millise jalajälje sa internetti jätad?
- Kuidas te oma isikuandmeid kaitsete?
- Kuidas kaitsete oma digiseadmeid?
- Mis on kahefaktoriline autentimine ja kus seda kasutada?

Otsige enda kohta infot Google abil.
Mida leidsite?

Lisalugemine

- **European Union. Agency for Network and Information Security** Review of Cyber Hygiene Practices, 2016
- **Gerardus Blokdyk**, Cyber Hygiene Third Edition, 2018
- **Gerardus Blokdyk**, Cyber Hygiene a Complete Guide - 2020 Edition



Lühivideod

- How is it easy to be hacked?
 - https://youtu.be/1hpU_Neg1KA
- What is a Digital Footprint?
 - <https://youtu.be/CfICOt2ul80>
- How to protect your data online
 - <https://youtu.be/XjJZoHOlgu4>
- What is Two-Factor Authentication (2FA)?
 - <https://youtu.be/mMKo-fG89jQ>
- A Data Breach Has My Data, What Do I Do?
 - <https://youtu.be/k5rIMr-u0Jw>
- Mobile Security Awareness
 - <https://youtu.be/ahNb6kA0Lms>



Tänan kuulamast!



Resources of pictures used in the presentation from:

- www.pixabay.com
- Personal archives

Screenshots made from websites